UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,753	11/21/2003	Alexander Hoffmann	16274.171	1445

22913 7590 08/26/2008

WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/718,753	**Applicant(s)** HOFFMANN, ALEXANDER	
	Examiner ABDULHAKIM NOBAHAR	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 07/10/2008.

2. Claims 1-35 are pending.

3. Claims 1, 13, 17, 18, 22-25, 29 and 32 are amended.

4. Applicant's arguments with respect to claims 1, 13, 22, 25, 29 and 32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas et al (US 2003/0072059 A1; hereinafter Thomas) in view of the applicant admitted prior knowledge described in the background section of the specification and hereinafter referred to as APK.

Regarding claims 1, 13, 25, 29, Thomas discloses:

a host (see, e.g., [0024]; Fig. 1; [0063]);

an interface electrically coupled to the host (see, e.g., Figs. 1 and 2; [0063]; and

A transceiver (see, e.g., [0039]; [0063]) comprising:

a transmitter configured to transmit data signals (see, e.g., [0068]);

a receiver configured to receive data signals (see, e.g., [0090]); and

a controller configured to encrypt a string and supply the encrypted string to a host to authenticate the transceiver (see, e.g., abstract; [006]; [0024]; [0066] and [0095], where the security system corresponds to the recited controller; [0115]; [0159]-[0160]; Fig. 11 and claim 24).

Thomas, however, does not expressly disclose:

authentication of the transceiver being contingent upon whether or not the transceiver has been certified by a manufacturer or supplier as meeting a specified quality standard (i.e., whether the transceiver is authentic or cloned).

APK discloses that manufacturers and suppliers have developed strict quality standards that must be met before their fiber optic transceivers are certified (i.e., authentic not cloned) for use in systems (specification, pages 1 and 2, paragraphs 3 through 6). Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement an authentication scheme to be contingent upon the authenticity of the transceiver as described in APK in the system of Thomas in order to prevent any harm to the users (see APK, page 4, 2nd paragraph).

Regarding claims 2 and 4, Thomas discloses:

The transceiver of claim 1, wherein the controller is configured to encrypt the string with a transceiver private encryption key (see, e.g., [0019]; [0063]; [0159]).

Regarding claims 3 and 28, Thomas discloses:The transceiver of claim 1, wherein the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver (see, e.g., [0030]; [0057]; [0159]; [0178]).

Regarding claim 5, Thomas discloses:

The transceiver of claim 3, wherein the transceiver public encryption key is sealed by encrypting the transceiver public encryption key with a system private encryption key and stored as a sealed transceiver public encryption key (see, e.g., [0031]; [0148]; [0159]-[0160]).

Regarding claim 6, Thomas discloses:

The transceiver of claim 5, wherein the sealed transceiver public encryption key is decrypted with a system public encryption key to retrieve the transceiver public encryption key (see, e.g., [0165]; [0186]).

Regarding claim 7, Thomas discloses:

The transceiver of claim 1, wherein the controller comprises an electrically erasable and programmable read only memory that is used to store a transceiver private encryption key and a transceiver public encryption key (see, e.g., [0147]-[0148]) .

Regarding claim 8, Thomas discloses:

The transceiver of claim 1, wherein the controller comprises a cryptography module for encrypting the string (see, e.g., [0066]).

Regarding claim 9, Thomas discloses:

The transceiver of claim 1, wherein the controller comprises an RSA encryption module for encrypting the string (see, e.g., [0159]).

Regarding claim 10, Thomas discloses:

The transceiver of claim 1, wherein the receiver comprises a fiber optic receiver (see, e.g., [0159]).

Regarding claim 11, Thomas discloses:

The transceiver of claim 1, wherein the transmitter comprises a fiber optic transmitter (see, e.g., [0003]; [0075]).

Regarding claim 12, Thomas discloses:

The transceiver of claim 1, wherein the transceiver comprises a small form factor pluggable transceiver (see, e.g., [0212], where in a wireless environment devices such as cellular phone, PDA and laptop are used, which use small form factor transceiver)

Regarding claim 14, Thomas discloses:

The network system of claim 13, wherein the interface comprises an inter-integrated circuit bus (see, e.g., [0063] and Fig. 1, where the devices of the network are connected electrically, thus their interface component of these devices are inter-integrated circuit buses).

Regarding claims 15 and 16, Thomas discloses:

The network system of claim 13, wherein the interface comprises a transceiver fault status line (see, e.g., [0179], where, for example, in case of a negative decision at step 1215 of Fig. 12 the “NO” branch is followed that will lead to the failure of cryptographic operation. This indicates that the system of Thomas has a mechanism for ending the communication which corresponds to the recited transceiver fault status line or disable line).

Regarding claim 17, Thomas discloses:

The network system of claim 13, wherein the interface comprises a transmit data in line TD+ and an inverted transmit data in line TD- (see, e.g., Figs. 1, 5 and 11, where the transmission and receiving lines for communication are shown).

Regarding claim 18, Thomas discloses:

The network system of claim 13, wherein the interface comprises a received data out line and an inverted received data out line (see, e.g., Figs. 1, 5 and 11, where the transmission and receiving lines for communication are shown).

Regarding claim 19, Thomas discloses:

The network system of claim 13, wherein the interface comprises a loss of signal status line (see, e.g., [0070]; 0203]; [0209]).

Regarding claim 20, Thomas discloses:

The network system of claim 13, wherein the host is one of a mainframe computer, a workstation, a server, and a storage device (see, e.g., [0071]; [0098]).

Regarding claim 21, Thomas discloses:

The network system of claim 13, wherein the host is one of a bridge, a router, a hub, a local area switch and a wide area switch (see, e.g., [0071]; [0085]; [0087]).

Regarding claim 22, Thomas discloses:

A transceiver (see, e.g., Figs. 4 and 11) comprising:

a transmitter configured and arranged to transmit data signals to an external device in response to commands from a host (see, e.g., [0068]; [0179], where authentication request corresponds to the recited command from the host);

a receiver configured and arranged to receive data signals from the external device and to pass corresponding data signals to the host (see, e.g., [0082]; [0090]; [0146], where the data signals are being converted); and

a controller in communication with the transmitter and the receiver and configured and arranged to communicate with the host to authenticate the transceiver with the host, wherein the controller stores a first unique transceiver-specific public key/private key pair for authentication (see, e.g., abstract; [0024]; [0115] and claim 24; [0159]; [0167]; 0178]).

Thomas discloses that the first unique transceiver-specific public key/private key may be assigned by the manufacturer of the transceiver (see [0167 and [0193]), but does not expressly disclose that the first unique transceiver-specific public key/private key corresponding with a manufacturer of the transceiver.

APK discloses that manufacturers and suppliers have developed strict quality standards that must be met before their fiber optic transceivers are certified (i.e., authentic not cloned) for use in systems (specification, pages 1 and 2, paragraphs 3 through 6). This indicates that that the transceiver's public key/private key pair should be assigned by the manufacturer to prove the transceiver authenticity. Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement an authentication scheme to be contingent upon the authenticity of the transceiver as described in APK in the system of Thomas in order to prevent any harm to the users (see APK, page 4, 2nd paragraph).

Regarding claim 23, Thomas discloses:

The transceiver of claim 22, wherein the first unique transceiver-specific public key/private key pair is associated with a first access code and the controller stores a second unique transceiver-specific public key/private key pair for authentication, wherein the second unique transceiver-specific public key/private key pair is associated with a second access code (see, e.g., [0034]; [0035], where the message type and object type identification correspond to the associated code).

Regarding claim 24, Thomas discloses:

The transceiver of claim 23, wherein the first unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the first access code to the controller and the second unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the second access code to the controller (see, e.g., [0159]-[0161]).

Regarding claims 26 and 27, Thomas discloses:

The fiber optic transceiver of claim 25, wherein the means for receiving data signals comprises means for converting optical serial data into electrical serial data (see, e.g., [0082]; [0146]).

Regarding claim 30, Thomas discloses:

The method of claim 29, wherein the authentication signal comprises a certificate identification (see, e.g., [0031]; [0035]).

Regarding claim 31, Thomas discloses:

The method of claim 29, wherein analyzing the authentication signal comprises decrypting the authentication signal using a public key of an issuing authority (see, e.g.,

[0165]).

Regarding claim 32, Thomas discloses:

A method for authenticating a transceiver, comprising:

installing a transceiver comprising a transceiver specific public key/private key pair, wherein the transceiver specific public key is encrypted with a private key of an issuing authority (see, e.g., [0159]; [0190];

electrically coupling the transceiver to a host through a communication link (see, e.g., Figs. 1 and 2; [0063]);

requesting the encrypted transceiver specific public key from the transceiver (see, e.g., [0159]; [0167]);

passing the encrypted transceiver specific public key from the transceiver to the host by way of the communication link (see, e.g., [0082]; [0160]); and

decrypting the encrypted (see, e.g., [0160]-[0161]).

Thomas does not expressly disclose that using a corresponding public key of the issuing authority to obtain the transceiver specific public key.

APK discloses that manufacturers and suppliers have developed strict quality standards that must be met before their fiber optic transceivers are certified (i.e., authentic not cloned) for use in systems (specification, pages 1 and 2, paragraphs 3 through 6). This indicates that that the transceiver’s public key/private key pair should be assigned by the manufacturer (or correspond to the manufacturer’s key pair) to prove the transceiver authenticity. Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement an authentication scheme to be contingent upon the authenticity of the transceiver as described in APK in the system of Thomas in order to prevent any harm to the users (see APK, page 4, 2nd paragraph).

Regarding claim 33, Thomas discloses:

The method of claim 32 comprising:

generating an original authentication string in the host;

sending the original authentication string from the host to the transceiver;

encrypting the original authentication string in the transceiver using the transceiver specific private key;

passing the encrypted authentication string from the transceiver to the host; and

decrypting the encrypted authentication string in the host using the transceiver specific public key. See Fig. 11 and the explanations in paragraphs [0159]-[0161].

Regarding claim 34, Thomas discloses:

The method of claim 33 comprising:

comparing the decrypted authentication string to the original authentication string; and

selecting one of rejecting and accepting the transceiver based upon the comparison. See paragraphs [0186] and [0187].

Regarding claim 35, Thomas discloses:

The method of claim 33, wherein the original authentication string is a random number (see, e.g., [0031]; [0160]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Abdulhakim Nobahar/
Examiner, Art Unit 2132

August 21, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132